UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/940,982	08/29/2001	Takashi Endo	NIT-295	5993

7590 10/03/2005

Mattingly, Stanger & Malur, P.C
1800 Diagonal Road, Suite 370
Alexandria, VA 22314

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 10/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/940,982	ENDO ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) *9-17* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 August 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *20010829*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

AT

DETAILED ACTION

Election/Restrictions

1. Applicant's election without traverse of Group I, Claims 1-8 in the reply filed on 15 July 2005 is acknowledged.

2. Claims 9-17 are withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a nonelected invention, there being no allowable generic or linking claim. Election was made **without** traverse in the reply filed on 15 July 2005.

Drawings

3. Figures 1-4 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures.

4. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 206 (see Figure 2); 701 (see Figure 7); 801 (see Figure 8); 901-906 and 909-921 (see Figure 9); and 1001 and 1010 (see Figure 10). Corrected drawing sheets

in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

5. The disclosure is objected to because of the following informalities:

The specification appears to contain minor typographical and other errors. For example, on page 22, line 14, the phrase "the probability of appearance does not to be strictly 0.5" appears to be missing language. On page 27, lines 7 and 8, it appears "ransom" is intended to read "random".

Further, on pages 31-35, there appear to be discrepancies between the description of Figure 8 and the figure itself. For example, on page 31, lines 24-26, the description of step 808 in the specification states that the subscript of the array (b) is incremented; however, step 808 in Figure 8 shows b set equal to 0.

Appropriate correction is required. The above is not to be considered an exhaustive list of errors. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Double Patenting

6. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

7. Claims 1-8 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 14 of U.S. Patent No. 6615354 in view of Jaffe et al, US Patent 6510518.

Claim 14 of the conflicting patent is directed to a method that corresponds substantially to the apparatus claimed in Claims 1 and 2 of the present application. However, the conflicting patent does not explicitly disclose the limitation of Claim 1 that

the disturbance data and processed disturbance data each have a constant Hamming weight. Jaffe discloses that data used in cryptographic processing can be represented using a constant Hamming weight representation (column 4, line 55-column 5, line 30). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of the conflicting patent to include constant Hamming weight data, in order minimize the information leaked from cryptosystems by power consumption fluctuations (see Jaffe, column 2, lines 44-48). Claims 4 and 5 contain limitations similar to those of Claim 2, and thus correspond to limitations in Claim 14.

In reference to Claim 3, Jaffe further discloses that each bit has a logic value of 1 or 0 at a probability of 50% (see the table at column 9, noting the representations s_8; see also column 8, lines 41-45). In reference to Claim 6, Jaffe further discloses means for generating random numbers each having a Hamming weight equal to half the numbers of bits include in the random number, means for inverting bits of data, and means for concatenating a random number with data output by the means for inverting (see the table at column 9, noting the representations s_8; see also column 8, lines 41-45). In reference to Claim 7, Jaffe further discloses a Hamming weight computation means, a Hamming weight examination means, and a constant Hamming weight assurance means (see column 4, line 55-column 5, line 30, where the representations guarantee a constant Hamming weight). In reference to Claim 8, Jaffe further discloses means used to generate partial random numbers with uniform bit counts and means for concatenating the partial random numbers to result in a final random number (see the

table at column 9; Figure 1; and column 7, line 57-column 8, line 65). Therefore it would have been obvious to further include the limitations of Jaffe for the reasons set forth above in reference to Claims 1 and 2.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 1-8 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "all but constant" in claims 1 and 4 is a relative term which renders the claim indefinite. The term "all but constant" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. The specification never sets forth how close to constant a signal or value must be to be considered "all but constant".

The term "all but uniform" in claim 5 is a relative term which renders the claim indefinite. The term "all but uniform" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. The specification never sets forth how close to uniform a signal or value must be to be

considered "all but uniform", nor does the specification even explicitly include the phrase "all but uniform".

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant admitted prior art in view of Jaffe et al, US Patent 6510518.

In reference to Claim 1, Applicant admits as prior art an apparatus including a data transform means transforming input data by using disturbance data to generate transformed data, a transformed data processing means for carrying out predetermined processing on the transformed data to generate processed transformed data, and a data inverse transform means for carrying out inverse transformation processing on the processed transformed data using processed disturbance data to generate processed data (see page 21, lines 1-12 of the present application). However, Applicant admits that such prior art does not explicitly disclose that the disturbance data and the processed disturbance data have a constant Hamming weight.

Jaffe discloses that data used in cryptographic processing can be represented using a constant Hamming weight representation (column 4, line 55-column 5, line 30). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of the prior art to include constant Hamming weight data, in order minimize the information leaked from cryptosystems by power consumption fluctuations (see Jaffe, column 2, lines 44-48).

In reference to Claim 2, Applicant admits that the prior art further discloses that the processed disturbance data can be generated by carrying out the predetermined processing on the disturbance data (page 21, lines 6-8 of the present application).

In reference to Claim 3, Jaffe further discloses that each bit has a logic value of 1 or 0 at a probability of 50% (see the table at column 9, noting the representations s_8; see also column 8, lines 41-45).

In reference to Claim 4, Applicant admits that the prior art further discloses generating processed disturbance data by carrying out the predetermined processing o the disturbance data (page 21, lines 6-8 of the present application). Further, it is well known that data can be pre-computed.

In reference to Claim 5, Applicant further admits that the processed disturbance data can be generated by carrying out the predetermined processing on the disturbance data (page 21, lines 6-8 of the present application).

In reference to Claim 6, Jaffe further discloses means for generating random numbers each having a Hamming weight equal to half the numbers of bits include in the random number, means for inverting bits of data, and means for concatenating a

random number with data output by the means for inverting (see the table at column 9, noting the representations s_8; see also column 8, lines 41-45).

In reference to Claim 7, Jaffe further discloses a Hamming weight computation means, a Hamming weight examination means, and a constant Hamming weight assurance means (see column 4, line 55-column 5, line 30, where the representations guarantee a constant Hamming weight).

In reference to Claim 8, Jaffe further discloses means used to generate partial random numbers with uniform bit counts and means for concatenating the partial random numbers to result in a final random number (see the table at column 9; Figure 1; and column 7, line 57-column 8, line 65).

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Kocher et al, US Patent 6278783, discloses cryptographic methods for smartcards, which are intended to prevent power analysis attacks, and which can include Hamming weight equalization.

b. Smart, "Physical Side-Channel Attacks on Cryptographic Systems", discloses various measures to protect against power analysis attacks, including balancing Hamming weights of operands.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER